

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF DELAWARE

WARNER BROS. ENTERTAINMENT
INC., a Delaware corporation;
TWENTIETH CENTURY FOX FILM
CORPORATION, a Delaware corporation;
COLUMBIA PICTURES INDUSTRIES,
INC., a Delaware corporation; SONY
PICTURES HOME ENTERTAINMENT
INC., a Delaware corporation; LIONS
GATE FILMS, INC., a Delaware
corporation; PARAMOUNT PICTURES
CORPORATION, a Delaware corporation;
and DISNEY ENTERPRISES, INC., a
Delaware corporation,

Plaintiffs,

vs.

DOES 1 - 9,

Defendants.

CIVIL ACTION No. 05-350

DECLARATION OF THOMAS CARPENTER IN SUPPORT OF PLAINTIFFS'
MOTION FOR LEAVE TO TAKE DISCOVERY PRIOR TO RULE 26(f)
CONFERENCE

I, Thomas Carpenter, declare:

1. I am Director, Data Services for MediaSentry, Inc. ("MediaSentry"), where I have been employed since January 2005. MediaSentry is a leading provider of online anti-piracy services for the motion picture, music, game and business software, and print publishing sectors. Before my employment with MediaSentry, I held various senior level positions at companies that developed Internet based technologies and have approximately ten years of experience related to the protocols, technical architecture and operation of the Internet.

2. I submit this declaration in support of Plaintiffs' Motion for Leave to Take Discovery Prior to Rule 26(f) Conference. This declaration is based on my personal knowledge, and if called upon to do so, I would be prepared to testify as to its truth and accuracy.

3. MediaSentry has developed a technology platform that provides an effective means to detect unauthorized distribution of digital music, software, games, content, and movies over online media distribution systems, or "peer-to-peer" ("P2P") networks. At MediaSentry, I am the head of the department that carries out evidence collection and provides litigation support services. I work closely with our development team to create credible techniques to scan for, detect, and download copies of copyrighted material on multiple network protocols for use by copyright owners.

4. MediaSentry was hired on behalf of Plaintiffs to monitor and identify copyright infringement of specified motion pictures on P2P networks. Under direct supervision of Plaintiffs' counsel, we engaged in a specific process utilizing specially designed software and other technology to identify direct infringers of Plaintiffs' copyrights on P2P networks.

5. Plaintiffs provided us with a list of copyrighted motion pictures they believe may be offered for distribution on P2P networks.

6. All of the users named as Doe Defendants were identified in one of two ways. We either: (1) searched for files corresponding to one of the motion picture titles on the list provided by the Plaintiffs and then identified the users who are offering the files; or (2) reviewed server logs obtained from P2P networks to determine the users who were offering the files. In the first identification method, we use the same core technical processes that are used by the P2P users on each respective network to identify users who are offering the specified motion picture files on the network, or to directly locate the specified files. In the second identification method, we reviewed the same data that would be available to the operator of a server that is part of the P2P network. Under the first method of identification, any user of a P2P network can obtain the information that is obtained by us from the P2P network. Under the second method of

identification, any operator of a server that is part of the P2P network can obtain the information that is obtained by us from the P2P network.

7. Once our searching software program identifies a file that it being offered for distribution that corresponds to one of the titles on the provided list of copyrighted motion pictures, or once such a file is identified directly from our search or our review of server logs, we obtain the Internet Protocol (“IP”) address of a user offering the file for download. When available, we also obtain the user’s pseudonym or network name and examine the user’s publicly available directory on his or her computer for other files that lexically match the motion pictures on Plaintiffs’ list. We then download at least one motion picture that the user is offering. In addition to the file of the motion picture itself, we download or otherwise collect publicly available information about the network user that is designed to help Plaintiffs identify the user. Among other things, we download or record for each file downloaded: (a) the time and date at which the file was distributed by the user; (b) the IP address assigned to each user at the time of infringement; and, in some cases, (c) the video file’s metadata (digital data about the file), such as title and file size, that is not part of the actual video content, but that is attached to the digital file and helps identify the content of the file. We then create evidence logs for each user that store all this information in a central database.

8. An IP address is a unique numerical identifier that is automatically assigned to a user by its Internet Service Provider (“ISP”) each time a user logs on to the network. Each time a subscriber logs on, he or she may be assigned a different IP address. ISPs are assigned certain blocks or ranges of IP addresses. ISPs keep track of the IP addresses assigned to its subscribers at any given moment and retain such “user logs” for a limited amount of time. These user logs provide the most accurate means to connect an infringer’s identity to its infringing activity.

9. Although users’ IP addresses are not automatically displayed on the P2P networks, any user’s IP address is readily identifiable from the packets of data being exchanged. The exact manner in which we determine a user’s IP address varies by P2P network.

10. An infringer's IP address is significant because it is a unique identifier that, along with the date and time of infringement, specifically identifies a particular computer using the Internet. However, the IP address does not enable us to ascertain with certainty the exact physical location of the computer or to determine the infringer's identity. It only enables us to trace the infringer's access to the Internet to a particular ISP and, in some instances, to a general geographic area. Subscribing to and setting up an account with an ISP is the most common and legitimate way for someone to gain access to the Internet. An ISP can be a telecommunications service provider such as Verizon, an Internet service provider such as America Online, a cable Internet service provider such as Comcast, or even an entity such as a university that is large enough to establish its own network and link directly to the Internet.

11. Here, the IP addresses identified enable us to determine which ISP was used by each infringer to gain access to the Internet. Publicly available databases located on the Internet list the IP address ranges assigned to various ISPs. However, some ISPs lease or otherwise allocate certain of their IP addresses to other unrelated, intermediary ISPs. Since these ISPs consequently have no direct relationship -- customer, contractual, or otherwise -- with the end-user, they are unable to identify the Doe Defendants through reference to their user logs. The intermediary ISPs' own user logs, however, should permit identification of the Doe Defendants.

12. Here, we determined that the Doe Defendants here were using Comcast Cable ("Comcast") to gain access to the Internet and distribute and make available for distribution and copying the copyrighted motion pictures identified. We downloaded the motion picture file and other identifying information described above and created evidence logs for each Doe Defendant. Once we identified the ISP used by the Doe Defendants to gain access to the Internet from the IP address, Plaintiffs' counsel, using the MediaSentry application, sent an e-mail to the relevant contact at Comcast informing Comcast of the Doe Defendant's IP address and the date and time of the infringing activity. That e-mail message requested that Comcast retain the records necessary to identify its subscriber who was assigned that IP address at that date and time. Once provided with the IP address, plus the date and time of the infringing activity, the Doe

Defendant's ISP quickly and easily can use its subscriber logs to identify the name and address of the ISP subscriber who was assigned that IP address at that date and time.

I declare under penalty of perjury that the foregoing is true and correct.

Executed on June 2, 2005, at Monistown, NJ


Thomas Carpenter